

LINUX Administrator's Quick Reference Card

Jialong He

Jialong_he@bigfoot.com

http://www.bigfoot.com/~jialong_he

User Management

Files

<code>/etc/group</code> <code>/etc/passwd</code> <code>/etc/shadow</code>	User account information.
<code>/etc/bashrc</code> <code>/etc/profile</code> <code>\$HOME/.bashrc</code> <code>\$HOME/.bash_profile</code>	BASH system wide and per user init files.
<code>/etc/csh.cshrc</code> <code>/etc/csh.login</code> <code>\$HOME/.cshrc</code> <code>\$HOME/.tcshrc</code> <code>\$HOME/.login</code>	TCSH system wide and per user init files.
<code>/etc/skel</code>	template files for new users.
<code>/etc/default</code>	default for certain commands.
<code>/etc/redhat-release</code> <code>/etc/slackware-version</code>	Redhat and Slackware version info (Linux kernel version with "uname -a")

Commands

<code>adduser</code>	script to create a new user interactively (slackware) or link to useradd (Redhat).
<code>useradd, userdel, usermod</code>	create, delete, modify a new user or update default new user information..
<code>newusers</code>	update and create new users (batch mode).
<code>groupadd, groupdel, groupmod</code>	add, delete or modify group.
<code>chage, chfn, chsh</code>	modify account policy (password length, expire data etc.) or finger information (full name, phone number etc.) change default login shell.
<code>linux init=/bin/sh rw</code>	gain root access during boot prompt without password, can be used to fix some problems. mount -w -n -o remount /

Network Configuration

Files

<code>/etc/rc.d/rc.inet1</code> (Slackware) <code>/etc/sysconfig/network-scripts/ifcfg-eth0</code> (Redhat)	IP address, Network mask, Default gateway are in these files. May edit manually to modify network parameters.
--	---

`/etc/HOSTNAME`
`/etc/NETWORKING` (Slackware)

hostname is set by "/bin/hostname" during boot and the name is read from these files. May change manually.

`/etc/sysconfig/network` (Redhat)

specify name server, DNS domain and search order. For Example:
search la.asu.edu
nameserver 129.219.17.200

`etc/resolv.conf`

`/etc/hosts`

host name to IP mapping file.

`/etc/host.conf`

host name information look up order. Example:
order hosts, bind
multi on

`/etc/nsswitch.conf`

new way to specify information source.

`/etc/networks`
`/etc/protocols`
`/etc/services`

TCP/IP services and ports mapping.

`/etc/rpc`

RPC service name to their program numbers mapping.

Commands

<code>netconfig</code>	menu driven Ethernet setup program.
<code>pppsetup</code>	setup PPP connection (Slackware). setup Ethernet during boot, for example <code>/sbin/ifconfig eth0 \${IPADDR} broadcast \${BROADCAST} netmask \${NETMASK}</code>
<code>ifconfig</code>	<code>/sbin/route add -net \${NETWORK} netmask \${NETMASK} eth0</code> <code>/sbin/route add default gw \${GATEWAY} netmask 0.0.0.0 metric 1</code>
<code>host</code>	lookup host name or IP (similar to nslookup).
<code>dnsdomainname</code>	show DNS domain name.
<code>arping; arp</code>	find out Ethernet address by first arping then arp.
<code>ipchains</code>	firewall and NAT (/etc/sysconfig/ipchains on Redhat)
<code>iptables</code>	firewall and NAT (/etc/sysconfig/iptables on Redhat)
<code>ntsysv</code>	menu driven SYSV service configuration (Redhat)
<code>chkconfig</code>	command line SYSV service configuration (Redhat)

Redhat files in /etc/sysconfig

Configuration Files

<code>keyboard</code>	keyboard map, e.g., KEYBOARD="/usr/lib/kdb/keytables/us.map"
<code>mouse</code>	Mouse type, e.g.,

MOUSETYPE=Microsoft
XEMU3=yes

network settings, contains
NETWORKING=yes
HOSTNAME=hostname.domain.com

network

NFS File Sharing

Files

<code>/etc/fstab</code>	file systems mounted during boot.
<code>/etc/exports</code>	NFS server export list.
<code>/etc/auto.master</code>	auto mount master file.

Commands

<code>mount</code>	mount a file system or all entries in fstab.
<code>exportfs</code>	export file system listed in exports
<code>showmount -e hostname</code>	show file systems exported

Printer Configuration

Files

<code>/etc/printcap</code> <code>/etc/printcap.local</code>	Printer capabilities data base.
<code>/etc/lpd.conf</code>	LPRng configuration file.
<code>/etc/lpd.perms</code>	permissions control file for the LPRng line printer spooler
<code>/etc/hosts.lpd</code>	Access control (BSD lpd).
<code>/etc/hosts.equiv</code>	trusted hosts.
<code>PRINTER</code>	Environment variable of default printer.
<code>/dev/lp0</code>	parallel port.

Commands

<code>lpc, lpq, lprm</code>	line printer control program, print queue maintain
-----------------------------	--

Sendmail

Files

<code>sendmail.cf</code> <code>sendmail.mc</code>	"sendmail.cf" is the configuration file. "sendmail.mc" is a macro file which can be used to generate "sendmail.cf" by: m4 sendmail.mc > sendmail.cf
<code>aliases</code>	mail aliases, must run "newaliases" after change. use :include: to include external list in a file.
<code>.forward</code>	per user aliases, use \yourname to prevent further expand and keeps a copy in mailbox.
<code>access</code>	mail access control, FEATURE(access_db) should be set

in sendmail.mc. For example, in /etc/mail/access
cyberpromo.com REJECT
mydomain.com RELAY
spam@somewhere.com DISCARD

makemap hash /etc/mail/access < /etc/mail/access

/etc/mail/relay-domains list all host/domain accepted for relaying.

Commands

newaliases rebuild the data base for the mail aliases file.
makemap build access database, e.g.,
makemap hash access.db<access

Useful Configuration Files

Files

httpd.conf Apache web server configuration file.
lilo.conf LILO boot loader configuration file.
syslog.conf System log daemon (syslogd) configuration.
ssh_config
sshd_config SSH client and server configuration files.
ld.so.conf default dynamic library search path (run ldconfig).
mttools.conf mtool configuration file (access DOS file).
named.conf DNS name server (BIND).
sysctl.conf kernel parameters by sysctl (Redhat).
ntp.conf net time server.
inetd.conf Internet super server.
Xinetd.conf, Xinet.d directory Extended inetd configuration.
proftpd.conf proftpd FTP server.
amanda.conf network backup server.
/etc/pine.conf
/etc/pine.conf.fixed PINE mail client system wide settings.

Rebuild Kernel

Configure Kernel Parameters

make config Unpack the tarball in /usr/src directory
make menuconfig bzip2 -dc linux-2.4.0.tar.bz2 | tar xvf -
make xconfig Configuring the kernel with interactive, menu or X window interface.

Compile Kernel Source

make dep Building and installing a new kernel.
make zImage cp arch/i386/boot/bzImage /boot/vmlinuz

Compile Modules

make modules
make modules_install Building and installing modules.

Manage Modules

insmod, lsmod, modinfo, modprobe, rmmod, depmod Manage loadable modules.

Miscellaneous

Files

/etc/shells allowed login shells
/etc/ftpusers user names NOT allowed to use ftp.
/etc/hosts.allow
/etc/hosts.deny TCP wrapper access control files.
/etc/sysconfig (redhat) contains system configuration files.
/dev/fd0 floppy drive A
/etc/inittab
/etc/init.d system run level control file.

Commands

fromdos, todos (Slackware)
dos2unix, unix2dos (Redhat) convert text file from/to linux format.
pwck, grpck verify integrity of password and group files.
pwconv, pwunconv, grpconv, grpuncov convert to and from shadow passwords and groups.
shadowconfig toggle shadow passwords on and off.
quota, edquota, quotacheck, quotaon, quotaoff, repquota, Manage disk quota.
lilo -D dos set LILO default OS (default=dos in lilo.conf)
ldd find out shared library dependencies.
lsuf list opened files.
fuser filename show processes that using the file.
ifdown ifup bring up/down a network interface (Redhat)

sysctl configure kernel parameters (Redhat).

socklist list opened socked.

shutdown [-r|h] now reboot / halt computer

nmap scan a host for opened ports.

crontab show or edit cron jobs.

sys-unconfig unconfigure system

chkconfig --list list services started at different run level.

unset TMOU disable BASH auto-logout feature

unset autologout disable TCSH auto-logout feature

kudzu probe for new hardware (Redhat).

rpm rpm -i INSTALL a package
rpm -e UNINSTALL a package
rpm -q QUERY a package
rpm -U UPDATE a package

man cmd | col -b >cmd.txt save a man page as a text file and remove control characters.

ntop -w 3000 Run **ntop** and listen on web port 3000. View traffic with browser to http://hostname:3000

Configure Apache 2.0 with SSL

mod_ssl

- (1) when compile apache, specify `--enable-ssl` for configure script. By default, ssl is not enabled. After compiling, use `"httpd -l"` to list the modules. "mod_ssl" should be in them.
- (2) generate private key with command:
openssl genrsa -out server.key 1024
- (3) generate certificate request
openssl req -new -key server.key -out server.csr
- (4) generate self-signed certificate
openssl x509 -req -days 60 -in server.csr -signkey server.key -out server.crt
- (5) modify "ssl.conf" which is included in "httpd.conf". Note, specify `"httpd -DSSL"`, otherwise, commented out `<IfDefine SSL>` in ssl.conf.

Syslog.conf

Each line consists of a selector and an action. A selector has two parts: facilities and priorities, separated by a period (.), You may precede every priority with an equation sign ("=") to specify only this single priority and not any of the above. You may also (both is valid, too) precede the priority with an exclamation mark ("!") to ignore all that priorities, either exact this one or this and any higher priority.

Example:
 mail.notice /var/log/mail # log to a file
 *.emerg @myhost.mydomain.org # log to remote host

Note: separator between first column and second column (log file name) must be TAB, not spaces.

facilities auth, auth-priv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, local0 – local7.

priorities debug, info, notice, warning, err, crit, alert, emerg.

action

Regular File:
File with full pathname beginning with “/”.

Terminal and Console:
Specify a tty, same with /dev/console.

Remote Machine:
@myhost.mydomain.org

Samba File and Printer Sharing

Introduction

Samba provides file and printer sharing with MS Windows computers. It makes UNIX speaks SMB/ICFS file and printer sharing protocol. The latest version of samba can be downloaded from

<http://www.samba.org>.

Samba is controlled by a configuration file “smb.conf”. On Redhat Linux, one can use “**redhat-config-samba**” to modify the configuration file. On other systems, SWAT is a web based GUI interface. SWAT is run from “inetd” and listen to port 901. You just need point your browser to <http://localhost:901> after starting swat.

Commands

- To test if the syntax of “smb.conf” is correct, use

testparm smb.conf

- List shares on a Samba or Windows server

smbclient -L machinename -U username

- Connect to a Samba or Windows server and get/put files using FTP like commands:

smbclient //machinename/sharename -U username

Security Mode in “smb.conf”

security = user

In this (default) security mode, samba maintain its own user login database which is usually in **/etc/samba/smbpasswd**. This file is created with command **/usr/sbin/smbpasswd**. Note, the user login file and command have the same name but in different directories. Following settings are used:
encrypt passwords = yes
smb passwd file = /etc/samba/smbpasswd

security = domain

In this security mode, samba server must join to an NT domain (using net command) and authenticate users by a domain controller. A user must have both valid UNIX and NT account in order to access files.

security = server

Use another computer (NT or W2k) to authenticate users. No need to join a domain. Need to specify a login server:
password server = mywin.domain.com

security = share

Give each share a password, no user name needed.

IPtables (Netfilter)

Command Syntax

iptables [-t <table >] <command> <chain > <parameters>

Save and Restore rules

/sbin/iptables-save > /etc/sysconfig/iptables
/sbin/iptables-restore < /etc/sysconfig/iptables

Firewall script sample

http://tiger.la.asu.edu/iptables_examples.htm

Build-in Table

filter This is the default table for handling network packets. Build-in chains are:

- INPUT** — This chain applies to packets received via a network interface.
- OUTPUT** — This chain applies to packets sent out via the same network interface which received the packets.
- FORWARD** — This chain applies to packets received on one network interface and sent out on another.

nat This table used to alter packets that create a new connection. Build-in chains:

- PREROUTING** — This chain alters packets received via a network interface when they arrive.
- OUTPUT** — This chain alters locally-generated packets before they are routed via a network interface.
- POSTROUTING** — This chain alters packets before they are sent out via a network interface.

Masquerade everything out ppp0.

iptables -t nat -A POSTROUTING -o ppp0 -j

MASQUERADE

Change source addresses to 1.2.3.4.

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 1.2.3.4

mangle

This table is used for specific types of packet alteration. Build-in chains:

- PREROUTING** — This chain alters packets received via a network interface before they are routed.
- OUTPUT** — This chain alters locally-generated packets before they are routed via a network interface.

Commands

--flush | -F Flush (delete) rules in the selected chain.

--policy | -P Set default policy for a particular chain.

--list | -L List all rules in filter table, use [-t tablename] to specify other tables.

--append | -A A appends a rule to the end of the specified chain.

-insert | -I Inserts a rule in a chain at a particular point.

Other commands:

(1) --new | -N (2) --delete | -D (3) --replace | -D (4) --zero | -Z (5) --check | -C (6) delete-chain | -X (7) rename-chain | -E

Parameters

--proto | -p [!] name protocol: by number or name, including **tcp, udp, icmp or all**.

--source | -s [!] addr/mask source IP address.

--destination | -d addr/mask destination IP address.

--in-interface | -i incoming interface name, e.g. eth0 or ppp0.

--out-interface | -o outgoing interface name.

--jump | -j jump to a particular target when matching a rule. Standard options: **ACCEPT, DROP, QUEUE, RETURN, REJECT**. May jump to a user defined chain.

--fragment | -f match second or further fragments only.

Options for TCP and UDP protocol

--sport | --source-port source and/or destination port. Can specify a range like 0:65535, use exclamation character (!) to NOT match ports.

--dport | destination-port

Options for TCP only

--syn Match SYN packets.

--tcp-flags Match TCP packets with specific bits set. For example, **-p tcp --tcp-flags ACK,FIN,SYN SYN** will only match TCP packets that have the SYN flag set and the ACK and FIN flags unset.

Options for ICMP only

--icmp-type [!] *type* Match specified ICMP type. Valid ICMP type can be list by
iptables -p icmp -h

Option for state module (-m state --state)

ESTABLISHED The matching packet is associated with other packets in an established connection.

RELATED The matching packet is starting a new connection related in some way to an existing connection.

NEW The matching packet is either creating a new connection or is part of a two-way connection not previously seen.

INVALID The matching packet cannot be tied to a known connection.

X Window (XFree86)

Files

To set screen resolution, in “Screen” section and Subsection “Display”, specify a mode. For example: Modes “1024x768”

To specify screen refresh rate, in “Monitor” section, specify vertical rate. For example: VertRefresh 70-120

\$HOME/.xinitrc
/etc/X11/xinit/xinitrc
/etc/X11/xinit/xinitrc.d scripts run after X server started
\$HOME/.Xclients
/etc/X11/xinit/Xclients

/etc/sysconfig/desktop decide which desktop (GNORM, KDE) to start (Redhat). (by /etc/X11/prefdm)

/etc/X11/fs/config configuration of X11 font path (font server).

Commands

startx start X window system.

Xconfigurator (Redhat)
xfree86setup (Slackware)
xf86config setup X server and generate XF86config.

XFree86 -configure XFree86 auto configuration (Plug-n-Play), generate a template named “XF86Config.new”

Ctrl+Alt+Del stop X server (on some system Ctrl+Alt+ESC).

Ctrl+Alt+F1
Ctrl+Alt+F7 F1 temporary switch to text mode, F7 switch back to graphic mode.

SuperProbe detect graphic hardware.

xvidtune adjust X server origin and size.

xmodmap modifying key map and mouse button map.

xhost server access control program for X.

xsetroot root window parameter setting utility for X.

xlsfonts server font list displayer for X.

xset ser preference utility for X.

XF86Config

XFree86 uses a configuration file called **XF86Config** for its initial setup. This file is normally located in “/etc/X11” or “/etc” directory. The XF86Config file is composed of a number of sections which may be present in any order. Each section has the form:

```
Section "SectionName"  
SectionEntry  
...  
EndSection
```

The graphics boards are described in the **Device** sections, and the monitors are described in the **Monitor** sections. They are bound together by a **Screen** section. Keyboard and Mouse are described in **InputDevice** sections, although *Keyboard* and *Pointer* are still recognized. **ServerLayout** section is at the highest level and bind together the InputDevice and Screen sections.

A special keyword called **Option** may be used to provide free-form data to various components of the server. The Option keyword takes either one or two string arguments. The first is the option name, and the optional second argument is the option value. All Option values must be enclosed in quotes.

File Section

FontPath "path"
Font path elements may be either absolute directory paths, or a font server identifier

RGBPath "path"
Sets the path name for the RGB color database.

ModulePath "path"
Allows you to set up multiple directories to use for storing modules loaded by the XFree86 server.

EXAMPLE

```
Section "Files"  
RgbPath "/usr/X11R6/lib/X11/rgb"  
FontPath "unix/:7100"  
EndSection
```

Serverflags Section

Option "DontZap" "boolean"
Disable use **Ctrl+Alt+Backspace** to terminate X server.

Option "DontZoom" "boolean"
Disable use ‘**Ctrl+Alt+Keypad +**’ and ‘**Ctrl+Alt+Keypad -**’ to switch video mode.

Option "BlankTime" "time"
Sets the inactivity timeout for the blanking phase of the screensaver in minutes. Default 10 min.

Option "StandbyTime" "time"
Sets the inactivity timeout for the "standby" phase of DPMS mode in minutes. Default 20 min.

Option "SuspendTime" "time"
Sets the inactivity timeout for the "suspend" phase of DPMS mode, default 30 min.

Option "OffTime" "time"
Sets the inactivity timeout for the "off" phase of DPMS mode, default 40 min.

Option "DefaultServerLayout" "layout_id"
Specify the default ServerLayout section to use. Default is the first ServerLayout section.

EXAMPLE

```
Section "ServerFlags"  
Option "BlankTime" "99999"  
Option "StandbyTime" "99999"  
Option "SuspendTime" "99999"  
Option "OffTime" "99999"  
EndSection
```

Module Section

Load "modulename"
Load a module. The module name given should be the module's standard name, not the module file name.

EXAMPLE

```
Section "Module"  
Load "extmod"  
Load "type1"  
EndSection
```

InputDevice Section

There are normally at least two InputDevice sections, one for Keyboard and one for Mouse.

Identifier
Specify an unique name for this input device.

Driver
Specify the name of the driver to use for this input device..

Option "CorePointer"
This input device is installed as the primary pointer device.

Option "CoreKeyboard"
This input device is the primary Keyboard.

EXAMPLE

```
Section "InputDevice"
  Identifier "Generic Keyboard"
  Driver "keyboard"
  Option "AutoRepeat" "500 30"
  Option "CoreKeyboard"
EndSection
```

```
Section "InputDevice"
  Identifier "PS2 Mouse"
  Driver "mouse"
  Option "CorePointer"
  Option "Device" "/dev/mouse"
  Option "Protocol" "PS/2"
  Option "Emulate3Buttons" "true"
EndSection
```

Device Section

Specifies information about the video card used by the system. You must have at least one Device section in your configuration file. The active device is in ServerLayout->Screen.

Identifier

Specify a unique name for this graphics card.

Driver

Specify the name of the driver to use for this graphics card.

EXAMPLE

```
Section "Device"
  Identifier "ATI Mach64"
  VendorName "ATI MACH64"
  VideoRam 2048
EndSection
```

Monitor Section

Monitor section describes a monitor. There must be at least one monitor section and the active one is used in ServerLayout->Screen.

Identifier

Specify a unique name for this monitor.

HorizSync horizsync-range

Gives the range(s) of horizontal sync frequencies of this monitor in kHz.

VertRefresh vertrefresh-range

Gives the range(s) of vertical sync frequencies of this monitor in Hz.

EXAMPLE

```
Section "Monitor"
  Identifier "Generic Monitor"
  VendorName "Monitor Vendor"
  ModelName "Monitor Model"
  HorizSync 31.5-56.6
  VertRefresh 40-70
EndSection
```

Screen Section

Screen Section binds Device and Monitor sections. There must be at least one Screen Section. The active one is in ServerLayout section.

Identifier

Specify a unique name for this Screen Section.

Device "device-id"

This specifies the Identifier of **Device section** to be used for this screen.

Monitor "monitor-id"

This specifies the Identifier of **Monitor section** to be used for this screen.

DefaultDepth depth

Default color depth, like 8, 16 or 24.

Option "Accel"

Enables XAA (X Acceleration Architecture), default is ON.

DISPLAY SUBSECTION

Each Screen section must have at least one Display Subsection which matches the depth values in DefaultDepth.

Depth depth

This entry specifies what color depth of this Display Subsection.

Virtual xdim ydim

Specifies the virtual screen resolution to be used.

ViewPort x0 y0

Sets the upper left corner of the initial display.

Modes "mode-name" ...

Specifies the list of video modes to use. Each mode-name specified must be in double quotes. They must correspond to those specified in the appropriate Monitor section (including implicitly referenced built-in ESA standard modes). mode can be switched with Ctrl+Alt+Keypad-Plus or Ctrl+Alt+Keypad-Minus.

EXAMPLE

```
Section "Screen"
  Identifier "My Screen"
  Device "ATI Mach64"
  Monitor "Generic Monitor"
  DefaultDepth 16
  SubSection "Display"
    Depth 16
    Modes "1024x768" "800x600" "640x480"
  EndSubSection
  SubSection "Display"
    Depth 24
    Modes "1024x768" "800x600" "640x480"
  EndSubSection
EndSection
```

ServerLayout Section

ServerLayout section binds a Screen section and one or more InputSection to form a complete configuration. The active ServerLayout section is specified in ServerFlags. If not, the first ServerLayout section is active. If no ServerLayout sections are present, the single active screen and two active (core) input devices are selected as described in the relevant sections.

Identifier

An unique name for this ServerLayout Section.

Screen screen-num "screen-id" position-information

The screen-id field is mandatory, and specifies the Screen section being referenced.

InputDevice "idev-id" "option" ...

Normally at least two are required, one for the core pointer and the other for the primary keyboard devices.

EXAMPLE

```
Section "ServerLayout"
  Identifier "Default Layout"
  Screen "My Screen"
  InputDevice "Generic Keyboard"
  InputDevice "PS/2 Mouse"
EndSection
```

Boot Sequences

Redhat

Usually the Linux kernel file is **/boot/vmlinuz** and is loaded by a boot loader (e.g., LILO). The first process created by the kernel is **/sbin/init**. It uses a configuration file **/etc/inittab**. init process runs **/etc/rc.d/rc.sysinit** script first, then runs all scripts in **/etc/rc.d/rc.N.d**, where *N* is the default run level defined in inittab. The actual scripts are stored in **/etc/rc.d/init.d** and proper links are created in run level directoris to point to corresponding scripts in initt.d directory. The last script to run is **/etc/rc.d/rc.local**.

Run level 1: Single user mode

Run level 3: Multiuser mode

Run level 5: Multiuser model with X11

Slackware

In Slackware, Linux kernel is **/boot/vmlinuz** and the first process started by the kernel is **/sbin/init**. Its configuration file is **/etc/inittab**. init first runs script **/etc/rc.d/rc.S**, then runs **/etc/rc.K** for single user mode or **/etc/rc.M** for multiuser mode. The last script to run is **/etc/rc.d/rc.local**.

rc.S calls scripts (**rc.modules**, **rc.pcmcia**, **rc.serial** and **rc.sysvinit**).

rc.M calls scripts (**rc.inet1**, **rc.inet2**, **rc.httpd**, **rc.samba**) and start some network server (lpd, httpd etc.)

rc.inet1 sets IP address, Mask, and default Gateway.

Run level 1: Single user mode

Run level 3: Multiuser mode

Run level 4: Multiuser model with X11